




EDUCAUSE

# Higher Education Research, Cybersecurity, and CMMC Compliance

# About

**EDUCAUSE** is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision-making at every level within higher education. A global nonprofit organization, EDUCAUSE members include US and international higher education institutions, corporations, not-for-profit organizations, and K-12 institutions. With a community of more than 85,000 individual participants located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation.

The **EDUCAUSE Cybersecurity Program** provides resources and events that are created by, and for, the higher ed information security, cybersecurity, and privacy communities. The program is informed and organized by an engaged, passionate, and experienced team of higher education information security and privacy professionals. An important part of the Cybersecurity Program is our EDUCAUSE member-led Higher Education Information Security Council (HEISC) that supports higher ed institutions as they improve information security governance, compliance, data protection, and privacy programs. HEISC accomplishes this work through volunteer groups supported by professional EDUCAUSE staff.

 **PreVeil** is built on MIT computer scientists' research on cybersecurity and applied cryptography. PreVeil strengthens the security of research data and files without sacrificing the openness and collaboration that serve as keystones of research enterprises. PreVeil enables researchers to work in a secure, CMMC and ITAR compliant environment, with collaborators from across multiple institutions joining at no cost. It makes encryption easy to use and deploy, without requiring changes in universities' existing IT infrastructures. PreVeil's encrypted email works with existing apps like Outlook or Gmail, letting users keep their regular email addresses. PreVeil Drive works like DropBox for file sharing, but with far better security. All messages and documents are encrypted end-to-end, which means that no one other than intended recipients can read or scan them—not even PreVeil. In addition, the system is designed with no central points of attack and therefore information cannot be stolen through compromised IT admins.

PreVeil supports compliance with virtually all of the CMMC mandates related to the communication and storage of CUI. Visit PreVeil's [CMMC page](#) to learn more.

# Higher Education Research, Cybersecurity, and CMMC Compliance

## Table of Contents

<b>4</b>	<b>Executive Summary</b>
<b>5</b>	<b>Introduction</b>
<b>6</b>	<b>CMMC Overview</b>
7	CMMC Levels
8	CMMC Model Framework
9	CMMC Domains
10	CMMC Process Maturity
11	CMMC Timing
<b>11</b>	<b>The CMMC Compliance Journey</b>
12	Understanding Key Cybersecurity Principles
14	First Steps to CMMC Compliance
18	Collaborating with Peers
20	CMMC Solutions
21	Case Studies
<b>24</b>	<b>Conclusion</b>
<b>25</b>	<b>Resources Appendix</b>
<b>27</b>	<b>About the Authors</b>
<b>28</b>	<b>Acknowledgements</b>
<b>29</b>	<b>Contacts</b>

# Executive Summary

**THE PURPOSE OF THIS BRIEF**—a joint effort on the part of EDUCAUSE and PreVeil—is to clarify the Department of Defense’s (DoD) new Cybersecurity Maturity Model Certification (CMMC) framework, and to guide your institution on its journey to CMMC compliance.

The DoD is taking a supply-chain risk-management approach to improving cybersecurity. That means that all 300,000 DoD contractors and researchers will need to obtain third-party certification that they meet requirements for the CMMC maturity level appropriate to the work they wish to do for the DoD. The new CMMC mandate includes university-based research labs and facilities—as well as FFDRCs (Federally Funded Research and Development Centers) and UARCs (University Affiliated Research Centers)—and thus CMMC compliance needs to be a part of your institution’s information security strategy.

This paper provides a high-level overview of the CMMC framework and its key components. It explains basic cybersecurity principles and how they connect with CMMC, and recommends first steps to take on your institution’s journey to CMMC compliance. That path will be made smoother by collaborating with your peers and learning from the work they’ve already done; several opportunities to do so are described herein. The paper culminates with a set of brief perspectives from research institutions outlining what they’re doing now to support cybersecurity for DoD research and CUI, and to position their institutions for CMMC compliance and certification. Resources to learn more are noted and hyperlinked throughout the paper; key resources are also compiled in the appendix.

It is important to note that implementation of the DoD’s CMMC framework is being closely watched by other federal agencies that also want to better secure CUI. These include NSF and NIH, which generally provide significantly more research dollars to universities than does the DoD. The Department of Education, too, is watching for possible applications for protecting student records; medical records subject to HIPAA also could be affected, along with student and alumni financial-related data.

Given the possible broad extension of the CMMC framework—or something quite similar—well beyond DoD research, it’s in your best interests to begin now to position your institution for CMMC compliance. It is our hope that this paper helps you do so. This is just the beginning of the CMMC journey: we will continue to work together to offer guidance as CMMC is implemented over the next few years.

# Introduction

In 2020, for an unprecedented fifth year in a row, information security came in at #1 on EDUCAUSE's Top 10 IT Issues list. Yet the 2020 results signal change: "information security" expanded to "information security strategy," reflecting a transition from more operational connotations to, as the EDUCAUSE Top 10 IT Issues Panel put it, "developing a risk-based security strategy that effectively detects, responds to, and prevents security threats and challenges."<sup>1</sup>

Formal information security strategies offer a path beyond managing day-to-day issues out of the IT office to more effectively addressing long-term challenges from a broader, institution-wide perspective. A broader approach is critical, as cybersecurity challenges abound in higher education. The openness and collaborative nature of universities is fundamental to their mission, but can complicate security efforts. Universities collect and retain sensitive data on students, parents, alumni, faculty and staff. The use of personal mobile phones, laptops and tablets among all these groups is widespread, risking exposure of sensitive information on less protected devices—a significant portion of which the institution may be unaware. To further complicate matters, many institutions have ties to hospitals, from small regional facilities to sprawling medical complexes, generating confidential medical records.<sup>2</sup>

Moreover, as an integral part of their missions, colleges and universities engage in research—much of it funded by the National Institutes of Health (NIH), the National Science Foundation (NSF), and the Department of Defense (DoD). This university-based research has long been the foundation of US global advantages in the medical, scientific, technological, military and commercial realms. It is no surprise, then, that the research presents a valuable target for cybercriminals, including well-funded state actors.

## Intellectual property a prime target of cyberattacks

In 2018, the US Department of Justice (DOJ) charged nine Iranian hackers in a three-year campaign of cyberattacks against hundreds of universities and private companies, pilfering more than \$3 billion worth of intellectual property (IP). Targets included nearly 150 US universities, where the hackers gained access to nearly 4,000 faculty email accounts, exfiltrating their contents and setting up auto-forwarding rules to themselves. The work was done by a Tehran-based organization, the Mabna Institute, the sole purpose of which, according to a DOJ attorney, is "to steal scientific resources from other countries around the world."<sup>3</sup>

In 2020, US security agencies have accused both China and Russia of sponsoring cyberattacks aimed at stealing IP related to the development and testing of Covid-19 vaccines—including research being done at universities.<sup>4</sup>

1 O'Brien, John. *Trees, Forests, and the 2020 Top 10 IT Issues*, EDUCAUSE Review: Jan. 27, 2020.

2 EDUCAUSE and Deloitte Center for Higher Education Excellence. *Elevating cybersecurity on the higher education leadership agenda*, Deloitte Insights: 2018.

3 Garrett M. Graff, "DOJ Indicts 9 Iranians for Brazen Cyberattacks against 144 US Universities," *Wired*, March 23, 2018

4 See: [U.S. accuses China of sponsoring criminal hackers targeting coronavirus research](#) and [U.S., Britain and Canada say Russian cyberspies are trying to steal coronavirus vaccine research](#). *Washington Post*, July 21, 2020 and July 16, 2020, respectively.

The Department of Defense spent \$105.3 billion on Research, Development, Test and Evaluation (RDT&E) in FY2020. That amount includes \$2.6 billion on basic research, over half of which was spent at universities.<sup>5</sup> EDUCAUSE's top IT issue—information security strategy—reflects the value of this research and illustrates higher education's close relationship with our nation's security interests.<sup>6</sup>

DoD is keenly aware of the cyber threats our nation faces and, indeed, is attacked 40 million times a day via the internet.<sup>7</sup> Clearly, as the EDUCAUSE Top 10 IT Issues Panel so aptly put it, "...the struggle to protect and secure information has become a forever war."<sup>8</sup>

A prime component of DoD's strategy in the forever cyber war is its newly created Cybersecurity Maturity Model Certification (CMMC) framework. The DoD created CMMC to better defend the vast attack surface it presents to adversaries. The US Defense Industrial Base (DIB) is comprised of more than 300,000 contractors and researchers throughout the country. Only about 1% of these organizations are primes; the remainder are subcontractors. Prime defense contractors are well protected, but subcontractors—which vary widely in terms of their size and cybersecurity capabilities—are the Achilles heel of the DIB. CMMC is designed to address that weakness and secure the DoD's supply chain, as summarized below.

## CMMC Overview

DoD is taking a supply-chain risk-management approach to improving cybersecurity.<sup>9</sup> That means that all 300,000 DoD contractors and researchers will need to obtain third-party certification that they meet requirements for the CMMC maturity level appropriate to the work they wish to do for the DoD.<sup>10</sup> This includes university-based research labs and facilities, as well as FFDRCs (Federally Funded Research and Development Centers) and UARCs (University Affiliated Research Centers). Thus CMMC compliance needs to be a part of your institution's information security strategy.

CMMC measures an organization's ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). FCI is information not intended for public release and is provided by or generated for the government under a contract to develop or deliver a product or service to the government. CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with federal law, regulations, and government-wide policies.

<sup>5</sup> Congressional Research Service: Federal Research and Development (R&D) Funding: FY 2020. Washington, DC. Updated March 18, 2020..

<sup>6</sup> Similarly, the Director of National Intelligence's annual Worldwide Threat Assessment report has for several years identified cyber threats as one of the most important strategic threats facing the United States. See: [www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf](https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf).

<sup>7</sup> See RSA blog by Admiral James Stavridis: [www.rsaconference.com/industry-topics/blog/new-department-of-defense-up-or-out-cybersecurity-standards-coming-fast](https://www.rsaconference.com/industry-topics/blog/new-department-of-defense-up-or-out-cybersecurity-standards-coming-fast)

<sup>8</sup> Grajek, Susan, and the 2019-2020 EDUCAUSE IT Issues Panel. *Top 10 IT Issues, 2020: The Drive to Digital Transformation Begins*, EDUCAUSE Review: Jan. 27, 2020.

<sup>9</sup> This CMMC overview, and the section that follows on cybersecurity principles relevant to CMMC, is largely excerpted from *Complying with the Department of Defense's Cybersecurity Maturity Model Certification (CMMC)*, published by PreVeil and updated regularly on its website.

<sup>10</sup> There are narrow exceptions to this requirement: According to the *OUSD(A&S) CMMC website's FAQs*, subcontractors need not be CMMC certified if they produce solely Commercial Off-The-Shelf (COTS) products. (See FAQ no. 20.) This applies, for example, to the supplier of chicken or fuel to a military installation, according to an analysis by Morrison & Foerster.

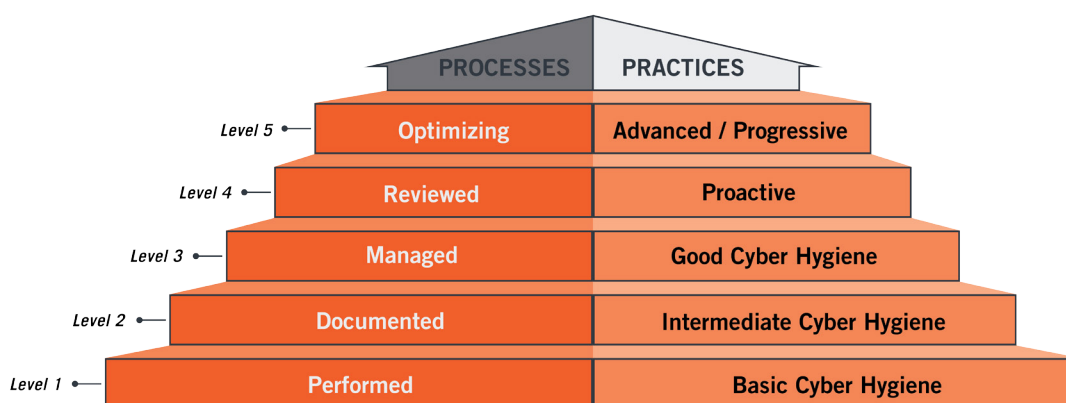
CMMC combines various cybersecurity standards already in place, and others, and maps these best practices and processes to five maturity levels ranging from basic cyber hygiene practices at Level 1 to highly advanced practices and processes at Level 5.

One of the most significant changes from previous practice is the shift from self-assessment to external assessments of cybersecurity compliance, which will be conducted by Third Party Assessment Organizations (C3PAOs). Further, whereas in the past noncompliance with DoD security regulations was acceptable as long as organizations prepared POAMS (Plan of Action and Milestones) outlining plans to address deficiencies, that will no longer be the case under CMMC.<sup>11</sup>

## CMMC Levels

CMMC's five defined levels of cybersecurity maturity, each with a set of supporting practices and processes, are shown in Figure 1 below. Practices range from basic cyber hygiene at Level 1 to advanced and progressive cyber hygiene at Level 5. In parallel, process levels range from simply performed at Level 1 to optimized at Level 5.

**Figure 1: CMMC Maturity Level Descriptions**



Source: CMMC Model 1.02, p. 4.

Note that university-based research labs, FFDRCs, and UARCs must meet requirements for the level they seek in both the practice and the process realms. For example, a research facility that achieves Level 3 on practice implementation and Level 1 on process institutionalization will be certified at the lower CMMC Level 1.

University researchers that work with or generate CUI need to achieve CMMC Level 3. The DoD explains:

An organization assessed at Level 3 will have demonstrated good cyber hygiene and effective implementation of controls that meet the security requirements of NIST SP 800-

<sup>11</sup> Organizations will still need to complete SSPs (System Security Plans), although those too will not satisfy CMMC requirements.

171 Rev 1<sup>12</sup>...Level 3 indicates a basic ability to protect and sustain an organization's assets and CUI... Note that organizations subject to DFARS Clause 252.204-7012<sup>13</sup> will have to meet additional requirement for Level 3, such as incident reporting.

For process maturity certification, a Level 3 organization is expected to adequately resource activities and review adherence to policy and procedures, demonstrating active management of practice implementation.<sup>14</sup>

## CMMC Model Framework

The CMMC model framework categorizes cybersecurity best practices into 17 broad domains, such as "Access Control" and "Systems and Communications Protection." Forty-three distinct capabilities, such as "control remote system access" and "control communications at system boundaries," are distributed across the 17 domains. Not all organizations need to demonstrate all 43 capabilities; they apply depending on the maturity level sought.

University researchers will demonstrate compliance with the required capabilities by showing adherence to a range of practices and processes. Practices are the technical activities required within any given capability requirement; 171 practices are mapped across the five CMMC maturity levels. Processes serve to measure the maturity of organizations' institutionalization of cybersecurity procedures; nine processes are mapped across the five CMMC maturity levels.

---

---

*One of the most significant changes from previous practice is the shift from self-assessment to external assessments of cybersecurity compliance, which will be conducted by Third Party Assessment Organizations (C3PAOs).*

---

---

12 NIST SP 800-171 Rev. 1 refers to a revision of the National Institute of Standards and Technology Special Publication 800-171, entitled Protecting CUI in Non-Federal Information Systems and Organizations. It codifies the requirements that any non-federal computer system must follow in order to store, process or transmit CUI or provide security protection for such systems.

13 DFARS Clause 252.204-7012 refers to a clause in a Defense Federal Acquisition Regulation Supplement entitled Safeguarding Covered Defense Information and Cyber Incident Reporting. It requires contractors to provide "adequate security" for covered defense information that is processed, stored or transmitted on the contractor's internal information system or network.

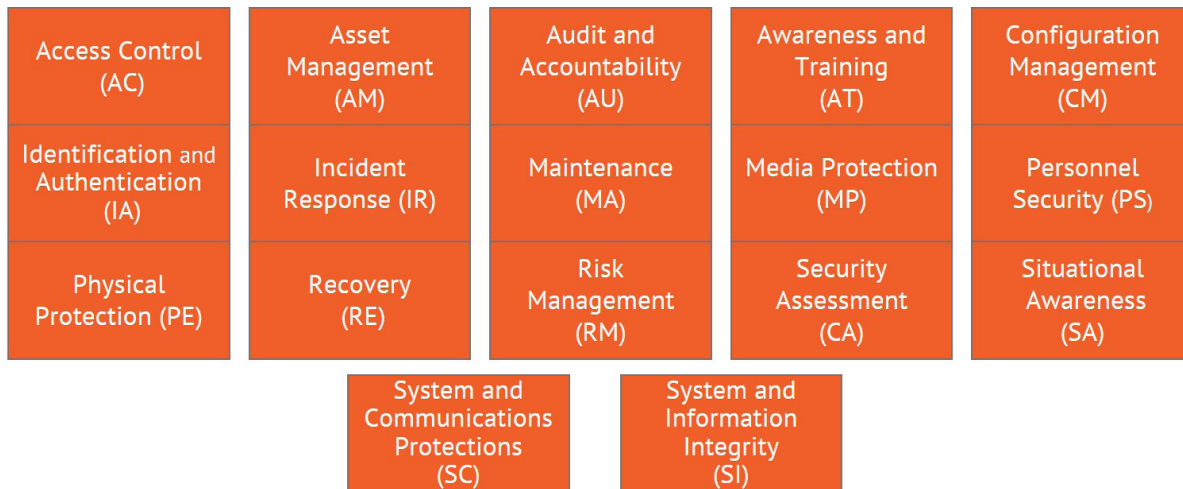
14 Office of the Undersecretary of Defense for Acquisition & Sustainment. Cybersecurity Maturity Model Certification, Version 0.7, p. 3. Accessed Feb. 2020.



## CMMC Domains

The CMMC model consists of 17 domains, shown in Figure 2 below, the majority of which originated from FIPS SP 200<sup>15</sup> security-related areas and the NIST SP 800-171 control families.

**Figure 2: CMMC Domains**



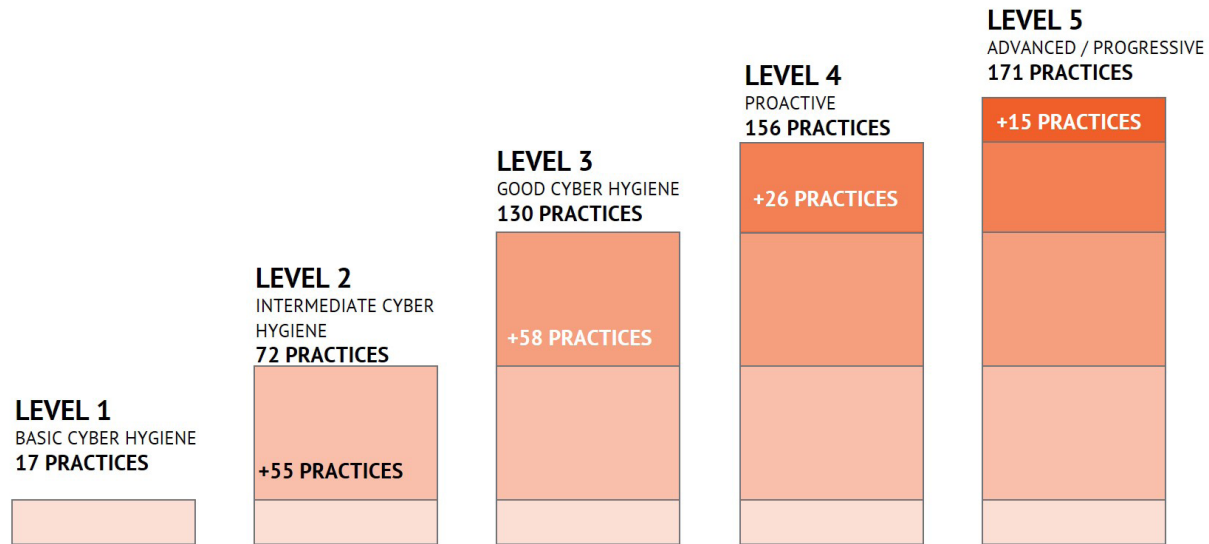
Source: CMMC Model 1.02, p. 7.

Again, 43 capabilities are distributed across these 17 CMMC domains, and the 171 practices associated with those capabilities are mapped across the five CMMC maturity levels.

An analysis of the practices by domains reveals that just six domains—Access Control; Audit and Accountability; Incident Response; Risk Management; System and Communications Protection; and System and Information Integrity—account for the majority of all practices (105 of 171). Figure 3 below shows how the practices accumulate as organizations move up the CMMC levels.

<sup>15</sup> FIPS 200 refers to the Federal Information Processing Standard Publication 200, entitled Minimum Security Requirements for Federal Information and Information Systems. It outlines mandatory federal standards for baseline security controls.

Figure 3: Practices per CMMC level



Source: CMMC Model 1.02, p. 10.

## CMMC Process Maturity

In addition to cybersecurity practices, CMMC will measure the maturity of organizations' institutionalization of cybersecurity processes. No maturity processes will be assessed at Level 1. Nine processes indicating increasingly more maturity are mapped across the remaining maturity levels, captured briefly as:

- Level 1: Performed (but no further process maturity requirements)
- Level 2: Documented
- Level 3: Managed
- Level 4: Reviewed
- Level 5: Optimized

Note that each required process applies to each domain individually. For example, the requirement that high-level management be informed of any issues within a domain requires 17 such formalized processes for doing so (given 17 domains).

Finally, adherence to CMMC practices and processes is cumulative. Once a practice or process is introduced in a level, it becomes required for all levels above that as well. Thus, for example, for an organization to achieve Level 3, all the practices and processes defined in Levels 1, 2 and 3 must be achieved. DoD prime contractors must flow down the appropriate CMMC level requirement to their subcontractors, which will vary depending on the nature of the subcontractors' work. For example, a prime contractor with CMMC Level 5 certification could have a subcontractor with which it shares just FCI; the DoD would require that subcontractor to achieve Level 1 certification.

## CMMC Timing

The speed of CMMC implementation has been somewhat dialed back from its original aggressive timeline as a result of the coronavirus pandemic. As of this publication, however, the DoD is still aiming to add CMMC requirements to RFPs in October 2020, starting with 15 procurements for critical DoD programs and technologies, such as those associated with nuclear and missile defense.<sup>16</sup> DoD expects that approximately 1,500 primes and subcontractors will be affected and, likewise, will need to be CMMC certified by Fall 2021. The roll-out will continue over a five-year period, with the expectation that all new DoD contracts will include CMMC requirements by Fall 2026. DoD will identify the required CMMC level in RFP sections L and M and use responses there as the basis of a “go/no go” decision.

The CMMC-Accreditation Body (CMMC-AB) is bearing much of the responsibility for implementation of the new framework. Standards and processes for licensing of individual assessors and certification of C3PAOs that will certify CMMC levels are being built from the ground up by the CMMC-AB. Ultimately, progress made by the CMMC-AB will determine the CMMC rollout timing. Stay abreast of developments on the [CMMC-AB](#) website.

# The CMMC Compliance Journey

This aim of the remainder of this paper is to offer a range of information and tips on achieving CMMC certification. We start with the basics by outlining key cybersecurity principles, an understanding of which can help your institution achieve CMMC certification. That brief primer is followed by advice on the first steps to take on the journey to CMMC compliance—which you’ve already begun if you’re reading this paper. Your path will be made smoother by collaborating with your peers and learning from the work they’ve already done; several opportunities to do so are described herein. Finally, this section culminates with a set of brief contributions from research institutions outlining what they’re doing now to support cybersecurity for DoD research and CUI, and to position their institutions for CMMC compliance and certification.

<sup>16</sup> Note that in July 2020, the US General Services Administration (GSA) released an RFP that refers to CMMC multiple times: “[The Streamlined Technology Acquisition Resources for Services \(STARS\) III Governmentwide Acquisition Contract \(GWAC\)—aka STARS III](#),” to provide IT services and IT service-based solutions. Section M.6 of the RFP states that bidders’ cybersecurity capabilities will be evaluated on a pass/fail basis, based on assessment of four elements, including: “The offerer’s intention in regards to obtaining Cyber [sic] Maturity Model Certification (CMMC), the target certification level, and a tentative timetable for attaining it.” Inclusion of CMMC in this RFP illustrates both the aggressive pace of CMMC implementation and its expected extension beyond DoD.

# Understanding Key Cybersecurity Principles

Cybersecurity research at leading universities has led to critical advances in applied cryptography. These new technologies, built on the fundamental security principles outlined below, will enable your institution to enhance its cybersecurity and will help it achieve the CMMC level necessary to do work for the DoD. Specific CMMC domains addressed by each security principle are noted.

## End-to-end encryption >>

End-to-end encryption ensures that data is encrypted on the sender's device and never decrypted anywhere other than on the recipient's device. This ensures that only the sender and the recipient can ever read the information being shared—and no one else. Data is never decrypted on the server, thus even if attackers successfully steal data from the server, it will be only encrypted gibberish.

>> **CMMC DOMAINS, END-TO-END ENCRYPTION** Access Control, Configuration Management, Media Protection, Systems & Communications Protection, and System & Informational Integrity.

## Encrypted logs >>

All user activities should be logged in order to trace possible malicious activities. Logs themselves also should be tamper-proof and protected with end-to-end encryption so that attackers cannot read sensitive files by viewing log entries, nor can they cover their tracks by deleting log entries.

>> **CMMC DOMAIN, ENCRYPTED LOGS** Audit & Accountability.

## Cloud-based services >>

Cloud-based services offer significant advantages over on-premises servers, such as lower costs, better scalability, and fewer administrative and maintenance responsibilities. However, many universities have been reluctant to trust sensitive information to the cloud. End-to-end encryption enables researchers to store sensitive information, like CUI, in the cloud because such information is always encrypted on the server. Further, the server can never access decryption keys. No one but the intended recipients can access the data, not even the cloud service provider.

>> **CMMC DOMAIN, CLOUD-BASED SERVICES** Maintenance & Recovery and Media Protection.

## Key-based authentication >>

Passwords create a significant security risk because they are routinely guessed or stolen. Compromised passwords are used for unauthorized access, escalating privileges, or impersonating a user's identity. A far better approach is to authenticate users with private keys that are stored only on the user's device. Unlike passwords, these keys cannot be guessed or stolen.

Moreover, device-based keys prevent hackers from remotely accessing user accounts. Since attackers cannot get to the keys, they cannot access data in users' accounts. If the devices are lost or stolen, device management controls should allow admins to quickly disable them.

### >> CMMC DOMAINS, KEY-BASED AUTHENTICATION

Identification & Access,  
System & Communications  
Protection, and Systems &  
Informational Integrity.

## Administrative distributed trust >>

In most IT systems, administrators hold the proverbial keys to the kingdom, given that they most often have access to any user account in the enterprise. As such, they become a central point of attack, and when an attacker compromises the administrator, they gain access to the entire organization's information.

A better approach is to require several people to approve an administrator's sensitive activities (such as exporting research data). Much like the nuclear launch keys, requiring several people to authorize critical actions can help prevent malicious activity. In essence, trust is distributed amongst approvers instead of being centralized with one admin. Distributed trust eliminates central points of attack.

It's also important to note that eliminating central points of attack is a fundamental means to secure systems. For example, some encryption systems centralize the storage of decryption keys in a key server. Doing so undermines the benefits of encryption because attackers can focus their efforts on penetrating the key server, which if successful would ultimately compromise all of the encrypted data.

>> CMCC DOMAINS,  
ADMINISTRATIVE  
DISTRIBUTED TRUST Access  
Control and Systems &  
Communications Protection.

## Controlled access >>

Many email and file sharing services are open to anyone, which enables phishing, spoofing, and other kinds of attacks. When an encrypted email and file sharing service is added to complement (instead of replace) regular email and files, access can be restricted to only trusted individuals. These people form a "trusted community" that allows organizations to control the flow of CUI. Individuals outside the trusted community are blocked from sending or receiving encrypted information.

>> CMMC DOMAINS,  
CONTROLLED ACCESS Access  
Control, Configuration  
Management, Systems &  
Communications Protection,  
and Systems & Informational  
Integrity.

## First Steps to CMMC Compliance

While CMMC is being phased in between now and Fall 2026, just when it will affect your institution depends upon the nature of the DoD research it conducts. Some institutions, such as those serving as subcontractors for primes working on critical DoD programs and technologies, may need to be CMMC certified as soon as Fall 2021. It appears likely that most others may have a two- or three-year window to achieve certification.

Again, one of the most significant changes from previous practice is the shift from self-assessment to external audits of cybersecurity compliance. Now is the time to begin to take initial steps so that when the time comes, your institution will be ready for its CMMC audit.

### **CMMC AB FAQs: Now is the time to start preparing for CMMC**

**Q.** If the CMMC standard is still in flux and there aren't any Assessors or C3PAOs, should an organization wait for the final standard to be available before it begins preparing for CMMC?

**A.** In short, **NO!** If your organization conducts business with the DoD and your contract includes the DFARS Clause 252.204.7012; you must comply with the guidance identified in NIST SP 800-171. Ensuring compliance with that current DFARS regulation has the benefit of easing compliance with CMMC when it is complete. We suggest organizations start preparation now.

## How to get moving

**Familiarize yourself with CMMC.** CMMC Model version 1.02 and its helpful, detailed appendices were released in mid-March 2020 and are available on the DoD's **CMMC** website. Stay abreast of developments, and use the official DoD site as your primary source of information.

**Determine responsibilities.** Some institutions have formed working groups to guide their CMMC strategies. One of the first tasks is to bring together the right people on campus— including directors of research compliance, export control, and contracts and grants; the vice chancellor for research; IT support; and the faculty senate—to both educate people about the new framework, and to determine who will be responsible for institutional CMMC compliance. A formal designation will empower that person and their office to move forward as needed.

**Determine the scope of CMMC for your institution, including all DoD-sponsored research currently being done.** A good place to start is with your grants and contracts office, to request information on all active DoD contracts the university has, including all research subject to FARS and DFARS Clause 252.204-7012. Ask for details about the amounts of the contracts, their timeframes, and renewal dates. The research office may not have this information already compiled; now is the time to do so.

**Next, determine the appropriate CMMC levels for the DoD research being conducted by your university.**

It appears most likely that research involving just FCI will need to achieve Level 1. Any research that involves CUI will need to achieve at least Level 3. Higher Levels 4 and 5 will focus on reducing the risk of advanced persistent threats (APTs) and are intended to protect CUI associated with DoD critical programs and technologies.<sup>17</sup>

### Extension of CMMC framework beyond DoD research

Not surprisingly, implementation of the DoD's CMMC framework is being closely watched by other federal agencies that also want to better secure CUI. In fact, CMMC requirements already have appeared in a General Services Administration (GSA) RFP for IT services (see footnote on p. 11). Other federal agencies keeping an eye on CMMC include NSF and NIH, which generally provide significantly more research dollars to universities than does the DoD. The Department of Education, too, is watching for possible applications for protecting student records; medical records subject to HIPAA also could be affected, along with student and alumni financial-related data.

Given the possible broad extension of the CMMC framework—or something quite similar—well beyond DoD, it's in your best interests to begin now to position your institution for CMMC certification.

**Conduct gap analyses.** Examine the current state of your cybersecurity and identify gaps between your organization's capabilities and the requirements for the CMMC level you seek.

This gap analysis could be based on previous self-assessments, such as the NIST SP 800-171 Self-Assessment. However, Table 1 below indicates the sources of CMMC practices by level, and shows that an analysis based on a NIST self-assessment would cover most—but not all—required practices for levels 2 and above. For example, Level 3 includes all of the security requirements in NIST SP 800-171, plus 20 other practices.<sup>18</sup>

Thus a more forward-looking approach would be to consult the **appendices of the CMMC Model 1.02 report**. Appendix A is organized by CMMC level. It includes a brief summary of the process requirements and a matrix that lists each domain's required capabilities and their corresponding practices by CMMC level, and also notes the sources for each practice in the model (e.g., FAR Clause 52.204-21, Draft NIST SP 800-171B, etc.).<sup>19</sup> The sources are helpful in that they enable you to cross check with compliance assessments that you have already undertaken. Ideally, you'll find that you are further along in the process than may first be apparent.

<sup>17</sup> Note that CMMC Level 2 is expected to serve largely as a transition in cybersecurity maturity progression from Level 1 to Level 3 (and the protection of CUI). That is, Level 2 is not expected to be used as a required level, but rather just as stepping stone.

<sup>18</sup> Note too that an institution that achieves CMMC Level 3 compliance is not necessarily DFARS Clause 252.204.7012 compliant. See **Understanding the role of DFARS in CMMC**.

<sup>19</sup> The "other" sources are referred to as "CMMC," which refers to cases in which the practice originated from contributors to the model—which includes DoD, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), members of the DIB, etc.—and not a previously published standard, reference or document.

**Table 1: Sources of CMMC practices by level**

CMMC Level	Number of Practices Introduced at CMMC Level	Source			
		48 CFR 52.204-21	NIST 800-171 r1	Draft NIST SP 800-171B	Others
1	17	15*	17*	-	-
2	55	-	48	-	7
3	58	-	45	-	13
4	26	-	-	11	15
5	15	-	-	4	11
Total	171	15	110	15	46

\*Note: 15 safeguarding requirements from 48 CFR 52.204-21 correspond to 17 security requirements in NIST SP 800-171.  
Source: CMMC Model 1.02, p.11.

### BYU Office of Computing Research CMMC assessment tool

Fortunately, you needn't be overwhelmed by mapping exercises flowing from the thorough—but likewise very dense—CMMC Model 1.02 appendices. Billy Wilson, of the Office of Research Computing at Brigham Young University (BYU), has created an enormously helpful **CMMC Assessment Tool** that captures all of the CMMC practice and process requirements. The spreadsheet has a Dashboard tab, where users choose the CMMC Level they want to achieve, which in turn affects the practices listed on each of the 17 following tabs—one for each domain. Users also choose which “reference family” (e.g., NIST 800-171) to show within each domain, depending on which will be most helpful for you to reference.

Under each domain tab, the user marks each required practice as not implemented, partially implemented, or fully implemented. Each required process is marked as performed, documented, managed, measured or optimized. The spreadsheet keeps a running tally of practices implemented and processes completed, with visual pies filling in as you work.

Clearly, gap analysis exercises will help you be ready to go and be first in line for a CMMC certification audit when the time comes.



**Engage with the CMMC-AB.** The CMMC-AB is chaired by Ty Scheiber of the Darden Executive Education School at the University of Virginia. Scheiber’s background in the defense and technology industries, as well as his current focus in higher education, positions the CMMC-AB well for spanning those realms and, importantly, for being receptive to input from higher education.

CMMC-AB has been conducting “national conversations” to share information and solicit input; currently, video recordings of four such conversations conducted in May 2020 are available on its website—as well as other important updates. You can subscribe to a CMMC-AB Alerts email list as well. Staying informed will help you and your colleagues contribute to the CMMC-AB’s deliberations and help ensure that higher education’s interests are effectively represented.

The **CMMC-AB** website, along with the DoD’s **CMMC** website, is a definitive source on implementation of the initiative. We recommend that these official sites serve as your primary source for all things CMMC.

## Higher Education: Ahead on NIST 800-171 compliance

According to a May 2019 report, *Reality Check: Defense industry’s implementation of NIST 800-171*,<sup>20</sup> universities lead the pack in NIST 800-171 compliance. Sera Brynn, a cybersecurity assessment firm, analyzed data compiled from two years of its compliance assessments and found that, on average, organizations had implemented just 39% of the NIST 800-171 controls—and none were 100% compliant. Analysis of results by size found that generally, the larger the company, the more robust the security environment. Analysis by industry was less predictable: Even compared to the most compliant industries, universities were in a league of their own, with 89% of controls implemented compared to the next best, i.e., software development (50%), manufacturing (46%), and aerospace (39%). One of the primary reasons noted for why universities are the most compliant environments is the high level of resources allocated for the security and protection of their research.

These results make clear what has long been true: Universities understand the critical importance of protecting CUI—not just related to research, but in its many forms such as student records, medical records, financial information, visas, and so on. And we have built effective processes and secure enclaves to comply with regulations governing that information. In short, cybersecurity is not a new concept for higher education; we have deep knowledge and expertise to offer federal agencies as they work to protect CUI across a wide range of organizations, industries and environments.

—Toby Smith, Vice President for Policy Association of American Universities (AAU)

20 Sera-Brynn. *Reality check: Defense industry’s implementation of NIST SP 800-171*. Sera-Brynn: May 2019.

***Finally, consider costs and funding mechanisms.***

As expected, costs of CMMC compliance are a serious concern throughout higher education. As your institution considers how to address its cybersecurity deficiencies, keep in mind that under CMMC, cybersecurity will continue to be an allowable F&A cost. This recognizes the critical nature of cybersecurity and supports CMMC compliance. You can begin now to build budgets for what it will take to upgrade your cybersecurity to the levels your institution needs to achieve, and figure out how those costs will affect your rates.

---

---

***As your institution considers how to address its cybersecurity deficiencies, keep in mind that under CMMC, cybersecurity will continue to be an allowable F&A cost. This recognizes the critical nature of cybersecurity and supports CMMC compliance.***

---

---

## **Collaborating with Peers**

National higher education associations also are working to better secure university research and to influence regulations governing federally-sponsored research. You can get involved at the national level to learn more, and to help foster improved regulations and better outcomes. A sampling of on-going, collaborative activities follows.

The AAU (Association of American Universities) and APLU (Association of Public Land-Grant Universities) Science & Security Working Group focuses on bolstering the security of the research they conduct—without sacrificing the openness and collaboration that serves as a keystone of their research enterprises.

AAU and APLU coordinate their efforts with other leading higher education associations, including ACE (American Council on Education), COGR (Council on Government Relations), and EDUCAUSE. For example, these five organizations submitted a joint comment to NIST on NIST SP 800-171B in August 2019 that requested several clarifications and concluded, “...we urge NIST to clearly state in the publication that these requirements are inappropriate for fundamental research activities.” Shortly after the groups shared their response to the proposed 800-171B guidelines with NIST, the agency announced that it was placing further development of the guidelines on hold pending completion of a related rule-making. The 800-171B process has remained on hold since that time, but the associations continue to watch for NIST efforts to revive it.

Other organizations that foster collaboration among higher education research institutions to secure research include **REN-ISAC** (Research and Education Networks Information Sharing and Analysis Center) and **Internet2**. EDUCAUSE works closely with both REN-ISAC and Internet2 on several important initiatives. If your institution isn't already involved with these organizations, you may wish to do so.

EDUCAUSE facilitates peer collaboration via its Community Groups (CGs), which are open, online communities led by members where you can share ideas and expertise, discuss solutions, and explore common interests. The CGs interact throughout the year via online discussions and most meet in-person at the EDUCAUSE Annual Conference. Two such groups may be of particular interest to readers wishing to share knowledge and stay abreast of CMMC developments, that is, the Higher Education Information Security Council—Governance, Risk and Compliance (HEISC-GRC) and the Security community groups. If you don't already subscribe to these groups, you can do so [here](#).<sup>21</sup>

Finally, the university research security community is sharing ideas and resources on a Slack channel, created in mid-2018. The channel, called **HigherEdCUI**, currently has nearly 200 participants. You can join to engage with peers, and share and learn strategies about securing CUI.

## Representing higher education

While the CMMC framework represents new opportunities and significant challenges for CISOs and their organizations, it's hard not to notice the absence of higher education in shaping the program. For many of us, the DoD is a major source of federal funding, yet the CMMC program is mute on the fundamental principle our research mission is founded upon: the free exchange of information. In a race to demonstrate cybersecurity rigor, defense contractors may overprescribe CMMC obligations, crippling the élan vital of modern science. Without clear guidance on controlling the contractual flow down of CMMC obligations, the program will greatly constrain the ability of DoD and defense contractors to benefit from our research capacity.

The long tail of science begins with the basic research performed in our myriad labs and computational enclaves. Basic research has long powered not just the national economy, but has advanced our national security aims as well. Our community must not watch the CMMC program as merely another regulatory schema to be imposed on us but rather—through our Vice-Presidents of Research and our Governmental Relations offices—we must aim to partner with DoD to build a better CMMC framework.

—Mike Corn, CISO, University of California, San Diego; Co-chair, EDUCAUSE HEISC

<sup>21</sup> A complete list of EDUCAUSE Community Groups is available [here](#).

## CMMC Solutions

Numerous companies focused on helping university researchers comply with NIST SP 800-171, DFARS Clause 252.204-7012, and other federal regulations have pivoted toward CMMC compliance services. A quick web search reveals a plethora of such offerings. It is important to note, though, that as of this publication no companies have been authorized to offer CMMC certification audits, despite claims being made otherwise. Indeed, the DoD has posted a clarification on its CMMC website to confirm that “...there are no third-party entities at this time that have been credentialed to conduct a CMMC assessment which will be accepted by the CMMC Accreditation Body.”

That said, the CMMC-AB notes on its site that “...offering pre-assessments or consulting using the most current draft of the [CMMC] standard is acceptable and encouraged.” Numerous such assessments are currently being offered by a wide range of companies; a review of those is beyond the scope of this paper.

With regard to CMMC’s process maturity side, each required process applies to each domain individually. Again, for example, the requirement that high-level management be informed of any security issues within a domain requires 17 such formalized processes and policies for doing so (given 17 domains). Once processes and policies are developed and formalized, the work to extend them across the CMMC domains could be repetitive. In that case, starting with templates for such policies, which can be customized for your institution, could save time and expense.

---

---

***As of this publication no companies have been authorized to offer CMMC certification audits, despite claims being made otherwise.***

---

---

CMMC’s 171 practices span 43 capabilities across 17 domains—and likewise have spawned solutions that span a wide range of CMMC requirements. Companies offering such solutions should be able to readily identify the CMMC requirements their products satisfy. It is important to keep that consideration in mind when assessing vendors—along with compliance with other federal regulations relevant to your institution, such as FARS, DFARS, ITAR (International Traffic in Arms Regulations),<sup>22</sup> etc.

We understand how difficult it can be to navigate the vendor space. In response, in 2016, EDUCAUSE’s Higher Education Information Security Council (HEISC) partnered with Internet2 and REN-ISAC to create the **Higher Education Community Vendor Assessment Toolkit** (HECVAT). The toolkit is specifically designed for higher education to measure vendor risk. Before you purchase a third-party solution, ask the solution provider to complete a HECVAT questionnaire to confirm that information, data, and cybersecurity policies are in place to protect your sensitive institutional information and constituents’ PII. The advantage for solution providers is that the HECVAT can be used by multiple institutions to streamline procurement processes with their higher education clients.

---

<sup>22</sup> For details regarding ITAR regulations as updated in March 2020, see [PreVeil’s End-to-End Encryption Enables ITAR Compliance](#).

The EDUCAUSE Cybersecurity Program intends to monitor CMMC solutions and create a comprehensive resource, likely sorted by CMMC domain, over time. Until then, we will circulate information via EDUCAUSE's HEISC-GRC and Security Community Group listservs described above.

## Case Studies

To help guide your institution toward CMMC compliance, we reached out to a handful of university CISOs and research security and compliance officers, and asked:

*What are you doing now to support cybersecurity for DoD research and CUI that will position your institution for CMMC compliance and certification?*

Responses and preparedness, not surprisingly, reflected a range of possibilities—for example, on whether to set up research enclaves, or handle assessments of security environments in-house.

Here's what our contributors shared about their institution's journey to CMMC compliance:

### Purdue University

---

#### ***Carolyn Ellis, Cyber Security Research Program Manager***

Purdue University was quick to rally internally when conversations around CMMC started. Since June 2019, our Information Compliance, Export Control, and Research Computing staff has been regularly discussing CMMC and its impact on our very active role in aerospace & hypersonics research. After determining systems that Purdue intended to certify at what level, we performed an internal gap analysis. We documented gaps in our practices and processes while considering the level of security burden to researchers transitioning from fundamental research.

We have engaged in a third-party security audit to externally evaluate our cybersecurity posture and maturity. We recently kicked this engagement off, with it scoped to evaluate our alignment to the NIST Cybersecurity Framework and CMMC. We brought in central IT, distributed impacted IT, and regional campuses. While this will not be a certification, it will help us prepare for the upcoming steps.

Purdue's biggest challenge planning for CMMC has been the lack of a complete processes and timeline from the DoD and CMMC-AB. To be proactive, we are constantly sorting through factual, but incomplete, information and unofficial sources filling in the missing information with interpretations.

## Georgia Tech

---

### ***Blake Penn, Information Security Policy and Compliance Manager***

Georgia Tech is aware of the impending CMMC requirements and is adapting our current DFARS 7012 compliance strategy in order to address these. Unlike what we have heard from many other research universities, Georgia Tech has not created a centralized enclave for our CUI research projects. Instead, we have created an approach where we work with researchers within their existing research environments to develop a plan (SSP) for their environment to meet the NIST 800-171 requirements. After they sign off on the plan and perform any necessary remediation, we perform an assessment of their environment against their SSP and deliver a Report on Compliance (ROC) detailing our findings.

We have analyzed the requirements of the different CMMC levels and currently plan on using the same approach with CMMC. If we get a CMMC Level 3 contract, for example, then we plan on working with the researchers to develop an SSP to conform to those controls and then assess those controls (this should leave us well-prepared for an external audit). We have performed almost one hundred assessments over the past few years and given this experience are very comfortable with our processes.

Our only real concern is socializing additional requirements to the research community as the social change was our biggest challenge with DFARS 7012. Compliance fatigue is a potential problem with researchers who have only recently gotten used to the idea of research cybersecurity requirements.

## Indiana University

---

### ***Von Welch, Executive Director, IU Center for Applied Security Research (CACR)***

### ***Anurag Shankar, Senior Security Analyst, CACR***

To handle CUI, Indiana University will leverage its existing research cyberinfrastructure secured using the NIST Risk Management Framework (RMF) and NIST 800-53 controls (from which NIST 800-171 is derived). This approach has enabled us to provide HIPAA-compliant research computing for over a decade, and should be able to address CUI as well.

To prepare for CMMC, we are closely monitoring the CMMC Accreditation Board activities and CMMC Third Party Assessment Organization (C3PAO) program. For contracts without CUI, we are ready to apply for CMMC Level 1 certification now. For CUI, which will require CMMC Level 3 certification, we are waiting for details on the compliance criteria. Those criteria may necessitate costly CMMC enclaves and cloud infrastructures (for instance AWS GovCloud or Microsoft GCC High) that are already CMMC or FedRAMP certified.

Fortunately, the gradual rollout of CMMC over the next five years provides ample time to defer decisions until more information becomes available.

### *Tom Siu, CISO*

The pre-requisite CMMC certification will add a significant new set of costs to research universities interested in or currently supporting DoD sponsored research, particularly since self-assessment is not an option.

*On strategic decisions:* First, the institution's research strategy must be committed to pursuit of DoD sponsored research activities, and many will perform a cost-benefit calculation to determine if their organization has the will to implement these systems and processes to compete for the research contracts.

*On infrastructure:* Our institution has been supporting federally-sponsored research, from a cybersecurity and compliance perspective, for several years now. We built a research infrastructure enclave which is segmented away from the open academic and research network environments, effectively reducing the scope of the problem. The segmented environment permits an institution to apply more stringent cybersecurity controls and procedures to the research data and tools without constricting the other open IT environments.

When research proposals are evaluated by our research administration, those with contractual security controls are expected to be implemented in the secured research enclave, and therefore contracts and potential awards have been adapted to account for cost-sharing for this research environment infrastructure.

If we were to pursue CMMC certification for DoD sponsored research, we would adapt this research environment, which is already based on the NIST SP 800-171 control families, and add on the costs for CMMC assessment to research award negotiations.

Further, options for creating research enclaves include:

- Physically segmented server infrastructure, with virtual clients and controlled remote access capability.
- Cloud-based FedRAMP capable containers.
- If operating as subcontractors, institutional researchers could leverage an off-network service operated by the prime DoD contractor.

Contact information for each of the contributors above is available in the Resources Appendix. All are willing to discuss their approaches to CMMC compliance in more detail if you wish. For easier reference, the Resources Appendix also compiles the key resources and links offered throughout this paper.

# Conclusion

The CMMC framework is being rolled out in earnest. The CMMC-AB—the body bearing much of the responsibility for implementation of the new framework—recently opened registration for training for C3PAOs, the organizations that will conduct the external assessments needed for CMMC compliance. The first C3PAO class is expected to be certified in Summer 2020. CMMC requirements, which already have appeared in a General Services Administration (GSA) RFP for IT services, are expected to appear in DoD RFPs beginning in Fall 2020.

Universities, too, are addressing the CMMC framework in earnest. It is our hope that this brief has served to deepen your understanding of the new cybersecurity standards and helped you map a path forward to compliance. You needn't go it alone: Third-party solutions such as PreVeil, which leverage critical advances in cybersecurity and applied cryptography—particularly end-to-end encryption and distributed trust with no central point of attack—can help you reach the CMMC maturity level you need to achieve. And we cannot overstate the value of learning from your peers.

We also encourage you to actively engage with EDUCAUSE's Cybersecurity Program and its relevant Community Groups, as well as with the national organizations noted herein. Those organizations are working to represent higher education's interests as federal agencies—led by the DoD—increase cybersecurity regulations to protect our nation's global advantages in the medical, scientific, technological, military and commercial realms.

---

---

*Universities are addressing the CMMC framework in earnest. It is our hope that this brief has served to deepen your understanding of the new cybersecurity standards and helped you map a path forward to compliance.*

---

---



# Resources Appendix

This list includes top priority CMMC resources. Note that many additional resources are footnoted and/or hyperlinked throughout the paper.

- The definitive source of information regarding the CMMC framework is the Department of Defense's CMMC website: [www.acq.osd.mil/cmmc/index.html](http://www.acq.osd.mil/cmmc/index.html). The site includes a helpful [FAQ](#) section.
- The DoD CMMC website also posts the most up-to-date version of the DoD document, Cybersecurity Maturity Model Certification (CMMC), the most recent of which was released in March 2020. See: [www.acq.osd.mil/cmmc/docs/CMMC\\_ModelMain\\_V1.02\\_20200318.pdf](http://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf)
- The CMMC Accreditation Body (CMMC-AB) bears much of the responsibility for implementation of the new framework. The CMMC-AB website is an excellent source for staying up-to-date on the CMMC rollout: [www.cmmcab.org](http://www.cmmcab.org)
- PreVeil's white paper, [Complying with the Department of Defense's Cybersecurity Maturity Model Certification \(CMMC\)](#), offers a regularly-updated overview of the CMMC program.
- For more information about the EDUCAUSE Higher Education Information Security Council (HEISC) Advisory Committee see: [www.educause.edu/about/mission-and-organization/governance-and-leadership/member-committees/heisc-advisory-committee](http://www.educause.edu/about/mission-and-organization/governance-and-leadership/member-committees/heisc-advisory-committee)
- For more information about the EDUCAUSE Higher Education Community Vendor Assessment Toolkit (HECVAT) see: <https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit>
- BYU Office of Computing Research [CMMC assessment tool](#). The tool, an Excel spreadsheet, captures all of the CMMC practice and process requirements and keeps a running tally of practices implemented and processes completed, with visual pies filling in as you work.
- To join the HigherEdCUI slack channel, go to <https://slack.com/signin#/>, sign in, enter the name "HigherEdCUI," and join your colleagues.
- Additional copies of this paper can be downloaded at [University Research, Cybersecurity, and CMMC Compliance](#).

Finally, feel free to contact these case study contributors to learn more about their institutions' approaches to CMMC compliance:

- Carolyn Ellis, Cyber Security Research Program Manager, Purdue University: [carolynellis@purdue.edu](mailto:carolynellis@purdue.edu)
- Blake Penn, Information Security Policy and Compliance Manager, Georgia Tech: [blake.penn@security.gatech.edu](mailto:blake.penn@security.gatech.edu)
- Tom Siu, CISO, Case Western Reserve University: [thomas.siu@case.edu](mailto:thomas.siu@case.edu)
- Von Welch, Executive Director, IU Center for Applied Security Research (CACR), and Anurag Shankar, Senior Security Analyst, CACR, Indiana University: [vwelch@iu.edu](mailto:vwelch@iu.edu) and [ashankar@iu.edu](mailto:ashankar@iu.edu)

# About the Authors

**BRIAN KELLY** is director of the EDUCAUSE Cybersecurity Program. He has been an active member of the higher education information security community since 2007. He has participated on the EDUCAUSE Higher Education Information Security Council (HEISC) since 2009, serving on the Awareness and Training working group before joining the Security Professionals Conference Program Committee in 2015. Brian became vice chair of the conference in 2017 and chaired the 2018 Security Professionals Conference. Brian is also a member of the REN-ISAC community and several professional organizations, including the High Tech Crime Investigation Association (HTCIA) and Information Systems Audit Control Association. Brian was previously the Chief Information Security Officer at Quinnipiac University. His career in information security began with the United States Air Force in 1993; he is a retired Air Force Cyber Operations Officer. Brian earned a BS in Communication from the University of Connecticut and an MS in Information Assurance from Norwich University.

**RALUCA ADA POPA** is an assistant professor of computer science at UC Berkeley. Her research is in security and applied cryptography. Raluca has developed practical systems that protect data confidentially by computing over encrypted data, and has designed novel encryption schemes as well. She is co-founder and chief technology officer at PreVeil. Raluca earned her PhD in Computer Security, and two BS degrees, in Computer Science and Mathematics, from MIT. She is the recipient of several honors, including MIT 35 under 35; the Intel Early Career Faculty Honor Award; the George M. Sprowls Award for the best MIT Computer Science doctoral dissertation; a Google PhD Fellowship; and a Johnson award for the best MIT Computer Science Masters of Engineering thesis.

**SANJEEV VERMA** is co-founder and chairman of PreVeil. Sanjeev is a technology entrepreneur with a track record of building successful businesses. In 2000 he co-founded Airvana, which developed mobile wireless infrastructure used by leading mobile operators such as Verizon and Sprint to deliver high speed 3G data services. Airvana grew to become a large publicly traded company and the world's second-largest supplier of CDMA 3G mobile data infrastructure and the world's largest supplier of femtocell access points used to provide greater wireless coverage inside homes. Sanjeev serves on the advisory board of the MIT Sloan School of Management. He earned a BS in EE from the Delhi College of Engineering, an MS in EE from the University of Rhode Island, and an MBA from the MIT Sloan School of Management.

# Acknowledgements

In Spring 2020, PreVeil and EDUCAUSE recognized the need for clear information about CMMC and how universities can position themselves for CMMC certification, and so embarked on this project.

PreVeil and EDUCAUSE extend their thanks to:

- John O'Brien, EDUCAUSE President
- Susan Grajek, EDUCAUSE Vice President for Communities and Research
- Jarrett Cummings, EDUCAUSE Senior Advisor for Policy and Government Relations
- Members of the EDUCAUSE Higher Education Information Security Council, including particularly co-chair Michael Corn, CISO at University of California San Diego; Blake Penn, Information Security Policy and Compliance Manager at Georgia Tech; and Tom Siu, CISO at Case Western Reserve University.
- Randy Battat, PreVeil Co-founder and CEO
- Adm. Jim Stavridis, ret., former Supreme Allied Commander of NATO, former Dean of the Fletcher School of Law and Diplomacy at Tufts University, and PreVeil board member
- Maureen Devlin, higher education consultant

# Contacts

## Brian Kelly

Cybersecurity Program Director, EDUCAUSE  
282 Century Place Suite 5000  
Louisville, Colorado, 80027  
(303) 449-4430

[bkelly@educause.edu](mailto:bkelly@educause.edu)

 [@BKinCT](https://twitter.com/BKinCT)

## Raluca Ada Popa

Chief Technology Officer, PreVeil  
Robert E. and Beverly A. Brooks Assistant Professor  
UC Berkeley Dept. of Electrical Engineering  
and Computer Science

729 Soda Hall

Berkeley, CA 94720

[raluca@eecs.berkeley.edu](mailto:raluca@eecs.berkeley.edu)

 [@ralucaadapopa](https://twitter.com/ralucaadapopa)

## Sanjeev Verma

Chairman, PreVeil  
85 Devonshire Street, 8th Floor  
Boston, MA. 02109  
(857) 353-6480

[sanjeev@preveil.com](mailto:sanjeev@preveil.com)

 [www.linkedin.com/in/Sanjeev-Verma-PreVeil](https://www.linkedin.com/in/Sanjeev-Verma-PreVeil)

## Randy Battat

CEO, PreVeil  
85 Devonshire Street, 8th Floor  
Boston, MA. 02109  
(857) 353-6480

[rbattat@preveil.com](mailto:rbattat@preveil.com)

 [www.linkedin.com/in/randy-battat](https://www.linkedin.com/in/randy-battat)

## Nick Holda

Vice President, Revenue and Customer  
Operations, PreVeil  
85 Devonshire Street, 8th Floor  
Boston, MA. 02109  
(857) 353-6480

[nick@preveil.com](mailto:nick@preveil.com)

 [www.linkedin.com/in/nickholda/](https://www.linkedin.com/in/nickholda/)

## Jarret Cummings

Senior Advisor for Policy and Government  
Relations, EDUCAUSE  
1150 18th St NW #900  
Washington, District of Columbia, 20036-3846  
(202) 331-5372

[jcummings@educause.edu](mailto:jcumings@educause.edu)

 [@EDUCAUSEJarret](https://twitter.com/EDUCAUSEJarret)

